IN THE CLAIMS:

The text of all pending claims, (including withdrawn claims) is set forth below. Cancelled and not entered claims are indicated with claim number and status only. The claims as listed below show added text with underlining and deleted text with ~~strikethrough~~. The status of each claim is indicated with one of (original), (currently amended), (cancelled), (withdrawn), (new), (previously presented), or (not entered).

1. – 67 (CANCELLED)

67. (currently amended) An apparatus, comprising:

a virus scanner scanning a file stored in a storage device for infection with a virus;

a quarantining device quarantining the file from non-infected files on the storage device, when the file is infected; and

a converting device converting the quarantined file into encoded data by executing an encoding process that converts an infected file in an infected condition into another encoded data when the infected file is detected.

68.- 74. (cancelled)

75. (currently amended) An apparatus comprising:

a storage device storing a plurality of files and a status for each of the files indicating whether each of the files is infected with a virus;

an input device inputting a selected file with infected status;

a quarantining device quarantining the selected file on the storage device; and

a converting device converting the selected file into encoded data by executing an encoding process that converts an infected file in an infected condition into another encoded data when the infected file is detected.

76. - 78. (cancelled)

79. (currently amended) An apparatus, comprising:

a storage device storing a plurality of files and a status for each of the files indicating whether each of the files is infected with a virus;

an input device inputting a selected file to be converted; and

a converting device converting the selected file into encoded data by executing an encoding process that converts an infected file in an infected condition into another encoded data when the infected file is detected.

80.-83. (cancelled)

84. (currently amended) A method, comprising:

scanning a file for infection with a virus using a computer;

quarantining the file from non-infected files if the file is infected with a virus; and

converting the file into the encoded data, when infected. by executing an encoding process that converts an infected file in an infected condition into another encoded data when the infected file is detected

85.- 87. (cancelled)

88. (currently amended) A method, comprising:

storing a plurality of files and a status for each of the files indicating whether each of the files is infected with a virus;

inputting a selected file with infected status to be quarantined;

quarantining the selected file; and

converting the quarantined file into encoded data using a computer by executing an encoding process that converts an infected file in an infected condition into another encoded data when the infected file is detected.

89. (original) A method according to claim 88, wherein the file, when quarantined, is unable to be executed.

90.-91. (cancelled)

92. (currently amended) A method, comprising:

storing a plurality of files and a status for each file indicating whether the file is infected with a virus;

inputting a selected file to be encoded; and

converting the selected file into encoded data using a computer by executing an encoding process that converts an infected file in an infected condition into another encoded data when the infected file is detected.

93. (previously presented) A method according to claim 92, wherein the encoded data is unable to be executed.

94. (currently amended) A computer readable storage medium controlling a computer by:

scanning a file for infection with a virus;

quarantining the file if infected with a virus; and

converting the quarantined file into encoded data by executing an encoding process that converts an infected file in an infected condition into another encoded data when the infected file is detected.

95.- 100. (cancelled)

101. (currently amended) A computer readable storage medium controlling a computer by:

storing a plurality of files and a status for each of the files indicating whether each of the files is infected with a virus;

inputting a selected file with infected status to be quarantined;

quarantining the selected file; and

converting the quarantined file into encoded data by executing an encoding process that converts an infected file in an infected condition into another encoded data when the infected file is detected.

102.- 106. (cancelled)

107. (currently amended) A computer readable data structure controlling a computer, comprising:

a list of files stored on a storage device;

a virus status for each of the files indicating whether or not the file is virus infected; and

a quarantine status for each of the files indicated whether or not the file is quarantined, wherein the quarantined file is converted into encoded data by executing an encoding process that converts an infected file in an infected condition into another encoded data when the infected file is detected in the checking.

108. (cancelled)

109. (currently amended) A method comprising:

scanning a file for infection with a virus using a computer;

isolating the file from non-infected files, if the file is infected with a virus; and

converting the infected file into encoded data by executing an encoding process that converts an infected file in an infected condition into another encoded data when the infected file is detected.

110. (currently amended) An apparatus comprising:

a virus scanner detecting if a file is infected with a virus;

a saving unit saving a detected virus-infected file into a separate storage area for virus infected files; and

a converting unit converting the virus-infected file into encoded data by executing an encoding process that converts an infected file in an infected condition into another encoded data when the infected file is detected.

111. (NEW) A file processing method performed by an apparatus, the apparatus using a storage device, the storage device storing a plurality of files, the method comprising:

reading a file from the storage device;

checking whether or not the file is infected with a virus;

executing an encoding process that converts an infected file in an infected condition into another data when the infected file is detected in the checking; and

storing the converted data into the storage device.

112. (NEW) The file processing method according to claim 111, wherein the storing stores the converted data in a particular area on the storage device.

113. (NEW) The file processing method according to claim 112, wherein the particular

area is an area for quarantining an infected file from a non-infected file.

114. (NEW) The file processing method according to claim 111, wherein the converted data is kept in unexecutable state on the storage device.

115. (NEW) The file processing method according to claim 111, further comprising:
managing the converted data.

116. (NEW) The file processing method according to claim 115, wherein the managing includes deleting the converted file.

117. (NEW) A file processing method of a storage device, the storage device storing a plurality of files, the method comprising:
reading a file from the storage device;
checking whether or not the file is infected with a virus;
converting an infected file into other encoded data when the infected file is detected in the checking;
storing the encoded data into the storage device; and
restoring the encoded data back to the original state of the infected file before the infected file was converted, by reverse conversion.

118. (NEW) The file processing method according to claim 117, wherein the storing stores the encoded data in a particular area on the storage device.

119. (NEW) The file processing method according to claim 118, wherein the particular area is an area for quarantining an infected file from a non-infected file.

120. (NEW) The file processing method according to claim 117, wherein the encoded data is kept in unexecutable state on the storage device.

121. (NEW) The file processing method according to claim 117, further comprising:
managing the encoded data.

122. (NEW) The file processing method according to claim 121, wherein the managing

includes deleting the encoded file.

123. (NEW) A file processing method performed by a storage device, the storage device comprising a storage portion to store a plurality of files and a connector to be connect with another apparatus, the another apparatus using the plurality of files on the storage portion, the method comprising:

reading file from the storage portion;

checking whether or not the file is infected with a virus;

converting an infected file into other encoded data when the infected file is detected in the checking; and

storing the encoded data into a particular area on the storage portion.

124. (NEW) The file processing method according to claim 123, wherein the particular area is an area for quarantining an infected file from a non-infected file.

125. (NEW) The file processing method according to claim 123, wherein the encoded data is kept in unexecutable state on the particular area.

126. (NEW) The file processing method according to claim 123, further comprising:

managing the encoded data.

127. (NEW) The file processing method according to claim 126, wherein the managing includes deleting the encoded file.

128. (NEW) A computer-readable storage medium storing a program, which when executed by an apparatus, causes the apparatus to perform a method, the apparatus using a storage device, the storage device storing a plurality of files, the method comprising:

reading a file from the storage device;

checking whether or not the file is infected with a virus;

executing an encoding process that converts an infected file in an infected condition into another data when the infected file is detected in the checking; and

storing the converted data into the storage device.

129. (NEW) The computer-readable storage medium according to claim 128, wherein

the storing stores the converted data in a particular area on the storage device.

130. (NEW) The computer-readable storage medium according to claim 129, the particular area is an area for quarantining an infected file from a non-infected file.

131. (NEW) The computer-readable storage medium according to claim 128, the converted data is kept in unexecutable state on the storage device.

132. (NEW) The computer-readable storage medium according to claim 128, the method further comprising:

managing the converted data.

133. (NEW) The computer-readable storage medium according to claim 132, wherein the managing includes deleting the converted file.

134. (NEW) A computer-readable storage medium storing a program, the program causes an apparatus to perform a file processing method of a storage device, the storage device storing a plurality of files, the method comprising:

reading a file from the storage device;

checking whether or not the file is infected with a virus;

converting an infected file into other encoded data when the infected file is detected in the checking;

storing the encoded data into the storage device; and

restoring the encoded data back to the original state of the infected file before the infected file was converted, by reverse conversion.

135. (NEW) The computer-readable storage medium according to claim 134, wherein the storing stores the converted data in a particular area on the storage device.

136. (NEW) The computer-readable storage medium according to claim 135, wherein the particular area is an area for quarantining an infected file from a non-infected file.

137. (NEW) The computer-readable storage medium according to claim 134, wherein the encoded data is kept in unexecutable state on the storage device.

138. (NEW) The computer-readable storage medium according to claim 134, further comprising:

managing the encoded data.

139. (NEW) The computer-readable storage medium according to claim 138, wherein the managing includes deleting the encoded file.

140. (NEW) A computer-readable storage medium storing a program, which when executed by a storage device, causes the storage device to perform a method, the storage device storing a plurality of files, the method comprising:

reading a file form the storage portion;

checking whether or not the file is infected with a virus;

converting an infected file into other encoded data when the infected file is detected in the checking; and

storing the encoded data into a particular area on the storage portion.

141. (NEW) The computer-readable storage medium according to claim 140, wherein the particular area is an area for quarantining an infected file from a non-infected file.

142. (NEW) The computer-readable storage medium according to claim 140, wherein the encoded data is kept in unexecutable state on the particular area.

143. (NEW) The computer-readable storage medium according to claim 140, further comprising:

managing the encoded data.

144. (NEW) The computer-readable storage medium according to claim 143, wherein the managing includes deleting the encoded file.